PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :		(11) Internationale Veröffentlichungsnummer: WO 99/59292
H04L 12/22, 12/12, 29/06	A1	(43) Internationales Veröffentlichungsdatum: 18. November 1999 (18.11.99)

(21) Internationales Aktenzeichen: PCT/EP99/03088

(22) Internationales Anmeldedatum: 5. Mai 1999 (05.05.99)

(30) Prioritätsdaten:
198 20 765.4 8. Mai 1998 (08.05.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DR. WEISS GMBH [DE/DE]; Dossenheimer Weg, D–69198 Schriesheim (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: WEISS, Dieter [DE/DE]; Hertelsackerweg 1b, D–69250 Schriesheim (DE). KOHLMANN, Sigrid [DE/DE]; Hüttengasse 1a, D–69253 Heiligkreuzsteinach (DE).

(74) Anwalt: GEYER, Ulrich, F.; Wagner & Geyer, Gewürzmühlstrasse 5, D–80538 München (DE).

(81) Bestimmungsstaaten: JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: METHOD AND DEVICE FOR INCREASING DATA SECURITY IN DATA NETWORKS AND COMPUTERS

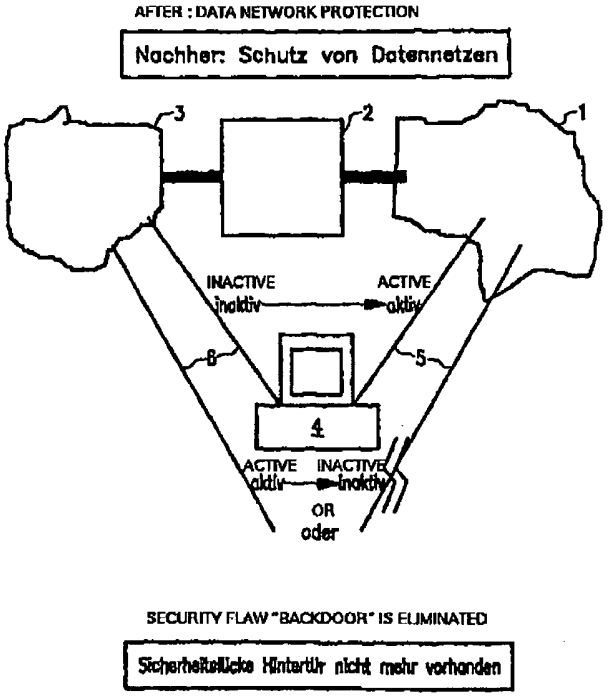
(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM ERHÖHEN DER DATENSICHERHEIT IN DATENNETZEN UND COMPUTERN

(57) Abstract

The invention relates to a method for increasing data security in a data network, according to which security flaws are reliably eliminated by physically deactivating at least one area of a data network to be protected by monitoring at least one communication channel. The invention also relates to a device for carrying out said method.

(57) Zusammenfassung

Bei einem Verfahren zum Erhöhen der Datensicherheit in einem Datennetz werden Sicherheitsmängel zuverlässig dadurch beseitigt, daß mindestens ein zu schützender Bereich in dem Datennetz durch die Überwachung wenigstens eines Kommunikationskanals physikalisch deaktiviert wird. Eine Vorrichtung zur Durchführung dieses Verfahrens ist angegeben.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Verfahren und Vorrichtung zum Erhöhen der Datensicherheit in Datennetzen und Computern

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zum Erhöhen der Datensicherheit und des Datenschutzes in Datennetzen und Computern.

Bei herkömmlichem Betrieb von Computern in Datennetzen werden Sicherungsverfahren, Überwachungen und Verriegelungen von Datenleitungen und Komponenten sowie auch Abschaltungen von Komponenten und aktiven Netzkomponenten durch Software Programme durchgeführt. Hierbei kommt meist ein Algorithmus mit Paßwort oder einer Verschlüsselung zur Sicherstellung des Datenschutzes zum Einsatz. Eine solche Absicherung ist jedoch hinsichtlich der Datensicherheit und des Datenschutzes problematisch, denn jedes Programm ist in Abhängigkeit vom eingesetzten Aufwand manipulierbar. Damit ist auch die Datensicherheit und der Datenschutz gefährdet. Nicht nur Firmen betreiben einen hohen Aufwand für die Sicherheit in ihren Datennetzen. Die Kommunikation zu anderen, fremden Datennetzen wird zum Beispiel oft an zentraler Stelle des Unternehmens mit Übergabeverbindungen (Gateways) geschaltet. Der Datenschutz wird hier meist über eine Softwarekomponente, einen sogenannten Firewall, sichergestellt. Die Sicherheit ist aber sofort außer Betrieb gesetzt, sobald ein hinter dem Firewall am Netz angeschlossener Computer einen weiteren externen Zugang in das zu sichernde Datennetz ermöglicht. Neuerdings werden Zugangssoftwareprogramme mit Kommunikationsprotokollen auf TCP/IP-Basis zur Kommunikation von Computern über Datennetze eingesetzt. Hierbei sind die Zugangspaßwörter oft auf Komponenten, zum Beispiel Festplatte, im kommunizierenden Computer gespeichert. Ist eine Kommunikation zum Beispiel in einem TCP/IP-Netz einmal aufgebaut, so ist der unbemerkte Aufbau einer anderen Verbindung aus dem Fremdnetz zum Computer nur mit viel Aufwand zu verhindern. Eindringende

Softwarepakete können den am Netz befindlichen Computer ausspähen, Daten verändern oder auch löschen. Somit besteht ein hohes Datenschutz- und Datensicherheitsrisiko.

Aus der DE 34 41 724 ist ein Verfahren zur Mißbrauchsverhinderung in Fernmeldenetzen, insbesondere in Mobilfunknetzen bekannt, mit dem die Sicherung einer Zentrale bzw. eines Datennetzes gegen Mißbrauch vorgenommen wird. Hierzu werden gerätespezifische Merkmale von Teilnehmergeräten und Benutzerkennungen überwacht. Im Falle eines wiederholten Mißbrauchsversuchs wird entweder die gerätespezifische Kennung zerstört oder betreffende Einträge in der Zentrale gelöscht. Durch diese Maßnahme wird das Datennetz immer als Ganzes geschützt. Das Verfahren ist weder dazu geeignet noch dazu vorgesehen, nach einem erfolgreichen Verbindungsaufbau zwischen dem Teilnehmergerät und der Zentrale oder dem Einwahlknoten diese gegen einen Mißbrauch innerhalb der Zentrale zu schützen bzw. einen Datenschutz der Zentrale zu gewährleisten. Das bekannte Verfahren betrifft nämlich nur den Verbindungsaufbau, nicht aber den Fluß der Dateninhalte.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zum Erhöhen der Datensicherheit und des Datenschutzes in Datennetzen und Computern anzugeben, bzw. zu schaffen, mit dem bzw. mit der die oben beschriebenen Sicherheitsmängel zuverlässig beseitigt werden.

Die gestellte Aufgabe wird dadurch gelöst, daß zu schützende Bereiche in einem Datennetz oder in einem Computer physikalisch deaktiviert werden. Die Deaktivierung erfolgt dabei durch die physikalische Blockierung der zu den zu schützenden Bereichen führenden Datenleitungen. Dazu wird mindestens eine Kommunikationsleitung überwacht und in Abhängigkeit vom Ergebnis der Überwachung physika-

lisch blockiert. Somit ist ein Eindringen in das Datennetzen unter Umgehen des Firewalls nicht mehr möglich. Ein Eindringen in den Computer wird zwar nicht verhindert. Durch eine Deaktivierung von wichtigen Komponenten des Computers wird der Datenschutz und die Datensicherheit jedoch bedeutend erhöht. Das Verfahren und die Vorrichtung erhöhen somit die Datensicherheit und den Datenschutz auch in Computern mit sensiblen Daten, wie sie zum Beispiel in Arztpraxen, Anwaltskanzleien und Behörden vorliegen.

Vorzugsweise werden mit dem Verfahren bzw. der Vorrichtung komplette Datennetzwerke, Teilnetzwerke, Computer oder Teilbereiche von Computern physikalisch deaktiviert. Die Deaktivierung dieser zu schützenden Bereich geschieht vorteilhafterweise durch die physikalische Blockierung der Datenleitungen, die zu den zu schützenden Bereichen führen. Die physikalische Blockierung kann dabei durch teilweise oder ganze Überbrückung, Trennung oder Ableitung erfolgen.

Vorzugsweise werden die Kommunikationsleitungen zu einem externen Datennetz während der Verbindung überwacht, wodurch abhängig vom Ergebnis der Überwachung der zu schützende Bereich deaktiviert wird. Die Überwachung der Datenleitungen kann dabei als primitive Überwachung, Verkehrsüberwachung oder Datenüberwachung erfolgen. Bei der primitiven Überwachung wird nur der Ruhezustand der zu überwachenden Leitungen überwacht. Alle Aktionen auf der Leitung (zum Beispiel Ruf, Sprache, Datenverkehr) führen zur Aktivierung des Schutzes des zu schützenden Bereiches. Bei der Verkehrsüberwachung wird der Verkehr auf der Leitung überwacht, wobei Signale zum Verbindungsaufbau (Ruf) ignoriert werden. Alle Aktionen auf der Leitung außer Ruf führen zu einer Aktivierung des Schutzes. Bei der Datenüberwachung werden bei einer digitalen Leitung Sprache und Daten analysiert. Eine Erkennung von Daten,

die nicht Sprachdaten sind, führt zur Aktivierung des Schutzes der zu schützenden Bereiche.

Eine weitere vorteilhafte Ausführungsform der Erfindung besteht darin, daß der zu schützende Bereich während der gesamten Zeit der Verbindung nach außen physikalisch deaktiviert wird. Eine weitere Erhöhung der Sicherheit kann dadurch erreicht werden, daß die physikalische Deaktivierung des zu schützenden Bereiches nach dem Abbau der Verbindung nach außen aufrecht erhalten bleibt. Dies kann zum Beispiel durch eine Zeitverzögerung erfolgen.

Vorteilhafterweise kann die Deaktivierung der zu schützenden Bereiche im einfachsten Fall durch Abschaltung der Energieversorgung für diese Bereiche erfolgen. Hierbei kann die Energieversorgung der zu überwachenden Funktionseinheit als externe Einspeisung erfolgen.

Gemäß einer anderen Ausführungsform der Erfindung wird die physikalische Deaktivierung des zu schützenden Bereiches visualisiert. Außerdem kann der Schutzzustand zum Beispiel durch Software ausgewertet werden, so daß diese auf einem eventuellen Angriff von außen reagieren kann.

Im folgenden wird ein Beispiel für den Einsatz des Verfahrens und der Vorrichtung gemäß der Erfindung zum Schutz vor Spionage eines Login-Paßwortes beschrieben. Emulationen, Terminalprogramme und Dekoder (wie zum Beispiel der T-Online Dekoder) speichern das Zugangspaßwort auf der Festplatte im Computer. Nach dem Aufbau einer Verbindung kann es vorkommen, daß diese Datei mit dem Paßwort über die Kommunikationsverbindung ausspioniert wird. Über das in der Erfindung beschrieben Sicherungsverfahren können die betroffenen Software Programme so modifiziert werden, daß diese Sicherheitslücke geschlossen wird. Hierzu muß die zu schützende Datei in dem zu schützenden Bereich abgelegt werden. Mit Start der Zu-

gangssoftware wird das Paßwort in den Arbeitsspeicher gelegt und die Verbindung zum externen Netz aufgebaut. Mit Beginn des Verbindungsaufbaus werden automatisch die zu schützenden Komponenten nach dem erfindungsgemäßen Verfahren funktionell außer Betrieb gesetzt. Als erste Maßnahme nach dem Einlog-Vorgang wird das Paßwort aus dem Speicher gelöscht. Der Paßwortschutz ist somit bedeutend sicherer geworden, da sich das Paßwort im geschützten Bereich befindet.

Ein anderes Beispiel für den praktischen Einsatz des erfindungsgemäßen Verfahrens wird nachfolgend anhand des Schutzes eines gesamten Computers beschrieben. Dabei wird das Betriebssystem eines Computers mit seinen unbedingt notwendigen Softwaremodulen beispielsweise auf eine kleine Festplatte, ROM-Disc oder in den Speicher geladen. Für den Datenaustausch kann ein ungeschützter Bereich im Computer belassen werden. Mit Beginn des Verbindungsaufbaus werden automatisch die zu schützenden Komponenten im Computer nach dem erfindungsgemäßen Verfahren funktionell außer Betrieb gesetzt. Eine sichere Kommunikation ist dadurch möglich.

Um die Datensicherheit und den Datenschutz weiter zu erhöhen, ist es erforderlich, eventuelle manuelle Manipulationen feststellen zu können. Als Zusatzverfahren zum Erhöhen des Datenschutzes und der Datensicherheit können zum Beispiel alle lösbaren Verbindungsteile oder anderweitige manipulierbare Komponenten des Netzes inklusive der Kommunikationsleitungen bis zum Computer über Plombierungen oder Siegelmarken abgesichert werden. Eine Plombierungsmethode ist die Absicherung über Siegelmarken, welche auf den lösbaren oder manipulierbaren Verbindungsteilen angebracht werden. Eine andere Plombierungsmethode kann aber auch ein Verhindern der Herstellung eines Kontaktes sein. Beim Lösen oder unbefugten Herstellen der Verbindung oder beim Entfernen der Siegelmarke wird

diese zerstört. Die Form, das Material und die Kennzeichnungsaufdrucke der Siegelmarke können beliebig gewählt werden. Eine weitere Plombierungsmethode ist die mechanische Verriegelung. So verfügen zum Beispiel Western- und RJ-Steckverbindungen über eine mechanische Nase, welche beim Herstellen der Verbindung einrastet. Die angebrachte Plombe verhindert das Niederdrücken der Nase an der Steckverbindung, so daß die Verbindung nicht gelöst werden kann.

Die technische Umsetzung des erfindungsgemäßen Verfahrens kann zum Beispiel als Netzschutzkomponente, externes Gerät oder als Einbaukomponente in einen Computer erfolgen. Unter Netzkomponenten werden einzelne Netzzugangskomponenten oder die Zusammenschaltung mehrerer Netzzugangskomponenten, wie zum Beispiel Anschlußdosen, verstanden. Die Überwachung und Abschaltung der Netzverbindung erfolgt direkt mit diesen Netzzugangskomponenten, die zum Beispiel in der Installationswand integriert werden. Jeder Computer kann somit direkt ohne weitere Maßnahme sicher an das Netz angeschaltet werden. Bei einem externen Gerät werden die verschiedenen Leitungen an das Schaltgerät geführt und die Schaltfunktion dort ausgeführt. Bei einer Einbaukomponente im Computer werden die überwachten und sichernden Leitungen/Netze direkt über eine Zusatzkomponente im Computer, wie zum Beispiel einem Modem oder einer Netzwerkbaugruppe geschaltet. Jeder Computer muß zur Nutzung dieser Methode zwar modifiziert werden, der Schutz ist aber nicht mehr räumlich gebunden, sondern wandert mit dem Standort des Computers.

Die Erfindung wird nachstehend anhand der Figuren 1 bis 5 erläutert.

Figur 1 zeigt ein Firmennetz 1, das über einen Firewall 2 mit dem Internet 3 verbunden ist. Der Firewall 2 dient dabei dem Schutz des Firmennetzes 1 vor Angriffen aus dem

Internet 3. Eine weitere Verbindung zwischen dem Firmennetz 1 und dem Internet 3 erfolgt über den Computer 4, wobei eine Leitung 5 das Firmennetz 1 mit dem Computer 4 verbindet. Eine Leitung 6 stellt die Verbindung zwischen dem Computer 4 und dem Internet 3 her. Da der Computer 4 einen weiteren externen Zugang zum Internet 3 darstellt, ist die über den Firewall 2 erreichte Datensicherheit des Firmennetzes 1 nicht mehr gegeben, sobald die Verbindungsleitung 6 zwischen dem Internet 3 und dem Computer 4 aktiv wird. Dieser Fall ist in Figur 5 dargestellt. Nach dem erfindungsgemäßen Verfahren wird jedoch die Verbindungsleitung 5 zwischen dem Computer 4 und dem Firmennetz 1 inaktiv, sobald die Verbindungsleitung 6 zwischen dem Internet 3 und dem Computer 4 aktiv ist. Dadurch ist das Firmennetz 1 vor Angriffen aus dem Internet geschützt. Solange die Verbindungsleitung 6 zwischen dem Internet 3 und dem Computer 4 inaktiv ist, kann die Verbindungsleitung 5 zwischen dem Computer 4 und dem Firmennetz 1 aktiv bleiben, da in diesem Fall keine Angriffsversuche aus dem Internet vorliegen.

Figur 2 zeigt das erfindungsgemäße Verfahren anhand des Schutzes einer Festplatte in einem Computer. Der Computer 7, der eine erste Festplatte 8 und eine zweite Festplatte 9 enthält, ist über die Leitung 10 mit dem Internet 3 verbunden. Sobald die Leitung 10 aktiv wird, d.h. Angriffsversuche aus dem Internet vorliegen, wird die zweite Festplatte 9 im Computer 7 physikalisch blockiert und somit deaktiviert.

Figur 3 zeigt einen an einem Kabel 12 befindlichen Stekker 13, der in der Buchse 14 steckt. Die Steckverbindung weist eine mechanische Nase 15 auf, die beim Herstellen der Verbindung einrastet. Die in Figur 3 gezeigte Plombe 17 verhindert das Niederdrücken dieser Nase an der Steckverbindung, so daß die Verbindung nicht gelöst werden kann. Bei manueller Manipulation der Steckverbindung wür-

de die in Fig. 3 gezeigte Plombe 17 und die in Fig.4 gezeigte Siegelmarke 16 zerstört werden.

Die Erfindung wurde zuvor anhand von bevorzugten Ausführungsbeispielen beschrieben. Dem Fachmann sind jedoch Ausgestaltungen, Modifikationen und Abwandlungen möglich, ohne daß dadurch der Erfindungsgedanke verlassen wird.

Patentansprüche

1. Verfahren zum Erhöhen der Datensicherheit in einem Datennetz, dadurch gekennzeichnet, daß mindestens ein zu schützender Bereich in dem Datennetz durch die Überwachung wenigstens eines Kommunikationskanals physikalisch deaktiviert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß mindestens ein komplettes Datennetzwerk, mindestens ein Teilnetzwerk in dem Datennetzwerk, mindestens ein Computer und/oder mindestens ein Teilbereich des Computers physikalisch deaktiviert wird.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die physikalische Deaktivierung des zu schützenden Bereiches durch eine physikalische Blockierung mindestens einer Funktionseinheit vorgenommen wird, die zu dem zu schützenden Bereich führt.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die Funktionseinheit durch eine mindestens teilweise Überbrückung des zu schützenden Bereiches physikalisch blockiert wird.

5. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die Funktionseinheit durch eine mindestens teilweise Trennung physikalisch blockiert wird.

6. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die Funktionseinheit durch eine mindestens teilweise Ableitung physikalisch blockiert wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Ruhezustand mindestens einer Datenleitung überwacht wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß mindestens eine Datenleitung verkehrsüberwacht wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Kommunikationsleitung insbesondere datenüberwacht wird.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die zu überwachende Funktionseinheit in Abhängigkeit vom Ergebnis der Überwachung physikalisch blockiert wird.

11. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der zu schützende Bereich während der gesamten Zeit der Verbindung nach außen physikalisch deaktiviert wird.

12. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die physikalische Deaktivierung des zu schützenden Bereiches nach dem Abbau einer Verbindung nach außen aufrechterhalten bleibt und durch eine berechtigte Funktionseinheit wieder aktiviert wird.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß die physikalischen Deaktivierung des zu schützenden Bereiches nach dem Abbau der Verbindung nach außen zeitverzögert aufrechterhalten bleibt.

14. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß eine Energieversorgung

für den zu schützenden Bereich in Abhängigkeit vom Überwachungsergebnis abgeschaltet wird.

15. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Zustand des zu schützenden Bereiches durch eine Software ausgewertet wird.

16. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Zustand der Aktivierung des zu schützenden Bereiches visualisiert wird.

17. Verfahren nach einem der vorhergehenden Ansprüche, das folgende Schritte umfaßt:

a) Starten einer Zugangssoftware für den Verbindungsaufbau zu einem externen Datennetz;
b) Laden eines Paßwortes in den zu schützenden Bereich eines Computers;
c) Aufbau einer Verbindung zu dem externen Datennetz;
d) Physikalische Deaktivierung des mindestens einen zu schützenden Bereiches.
e) Mitteilen des Paßwortes in dem externen Datennetz;
f) Löschen des Paßwortes aus dem Speicher;

18. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß Verbindungsschnittstellen zwischen lösbaren Verbindungsteilen mindesten eines Teils des Datennetzes plombiert werden.

19. Verfahren nach Anspruch 18, dadurch gekennzeichnet, daß die Verbindungsschnittstellen zwischen den lösbaren Verbindungsteilen des Datennetzes versiegelt werden.

20. Verfahren nach Anspruch 18, dadurch gekennzeichnet, daß die Herstellung eines Kontakts an den Verbindungsschnittstellen zwischen den lösbaren Verbindungsteilen des Datennetzes verhindert wird.

21. Verfahren nach Anspruch 18, dadurch gekennzeichnet, daß die Verbindungsschnittstellen zwischen den lösbaren Verbindungsteilen des Datennetzes mechanisch verriegelt werden.

22. Vorrichtung zum Erhöhen der Datensicherheit in einem Datennetz, dadurch gekennzeichnet, daß das Datennetz mindestens eine Einrichtung zum physikalischen Deaktivieren von mindestens einem zu schützenden Bereich in dem Datennetz aufweist.

23. Vorrichtung nach Anspruch 22, dadurch gekennzeichnet, daß der zu schützende Bereich mindestens ein komplettes Datennetzwerk, mindestens ein Teilnetzwerk in dem Datennetzwerk, mindestens ein Computer und/oder mindestens ein Teilbereich des Computers ist.

24. Vorrichtung nach Anspruch 22 oder 23, dadurch gekennzeichnet, daß die Deaktivierungseinrichtung mindestens eine Netzkomponente ist.

25. Vorrichtung nach Anspruch 24, dadurch gekennzeichnet, daß die Netzkomponente eine Netzzugangskomponente ist.

26. Vorrichtung nach Anspruch 25, dadurch gekennzeichnet, daß die Netzzugangskomponente mindestens eine Anschlußdose ist.

27. Vorrichtung nach Anspruch 22 oder 23, dadurch gekennzeichnet, daß die Deaktivierungseinrichtung ein externes Gerät ist.

28. Vorrichtung nach Anspruch 22 oder 23, dadurch gekennzeichnet, daß die Deaktivierungseinrichtung eine Einbaukomponente in einem Computer ist.

29. Vorrichtung nach Anspruch 28, dadurch gekennzeichnet, daß die Einbaukomponente eine Kommunikations-Baugruppe ist.

30. Vorrichtung nach einem der Ansprüche 22 bis 29, dadurch gekennzeichnet, daß der Computer eine Zeitverzögerungsschaltung zur Aufrechterhaltung der physikalischen Deaktivierung des zu schützenden Bereiches nach dem Abbau einer Verbindung nach außen aufweist.

31. Vorrichtung nach einem der Ansprüche 22 bis 30, dadurch gekennzeichnet, daß Schnittstellen zwischen lösbaren Verbindungsteilen oder manipulierbaren Teilen des Datennetzes Sicherungseinrichtungen aufweisen.

32. Vorrichtung nach Anspruch 31, dadurch gekennzeichnet, daß die Sicherungsmittel Plomben sind.

33. Vorrichtung nach Anspruch 31, dadurch gekennzeichnet, daß die Sicherungsmittel Siegelmarken sind.

34. Vorrichtung nach Anspruch 31, dadurch gekennzeichnet, daß die Sicherungsmittel mechanische Verriegelungen sind.

35. Vorrichtung nach Anspruch 31, dadurch gekennzeichnet, daß die Schnittstellen plombierte Steckverbindungen mit einer Arretierung aufweisen.

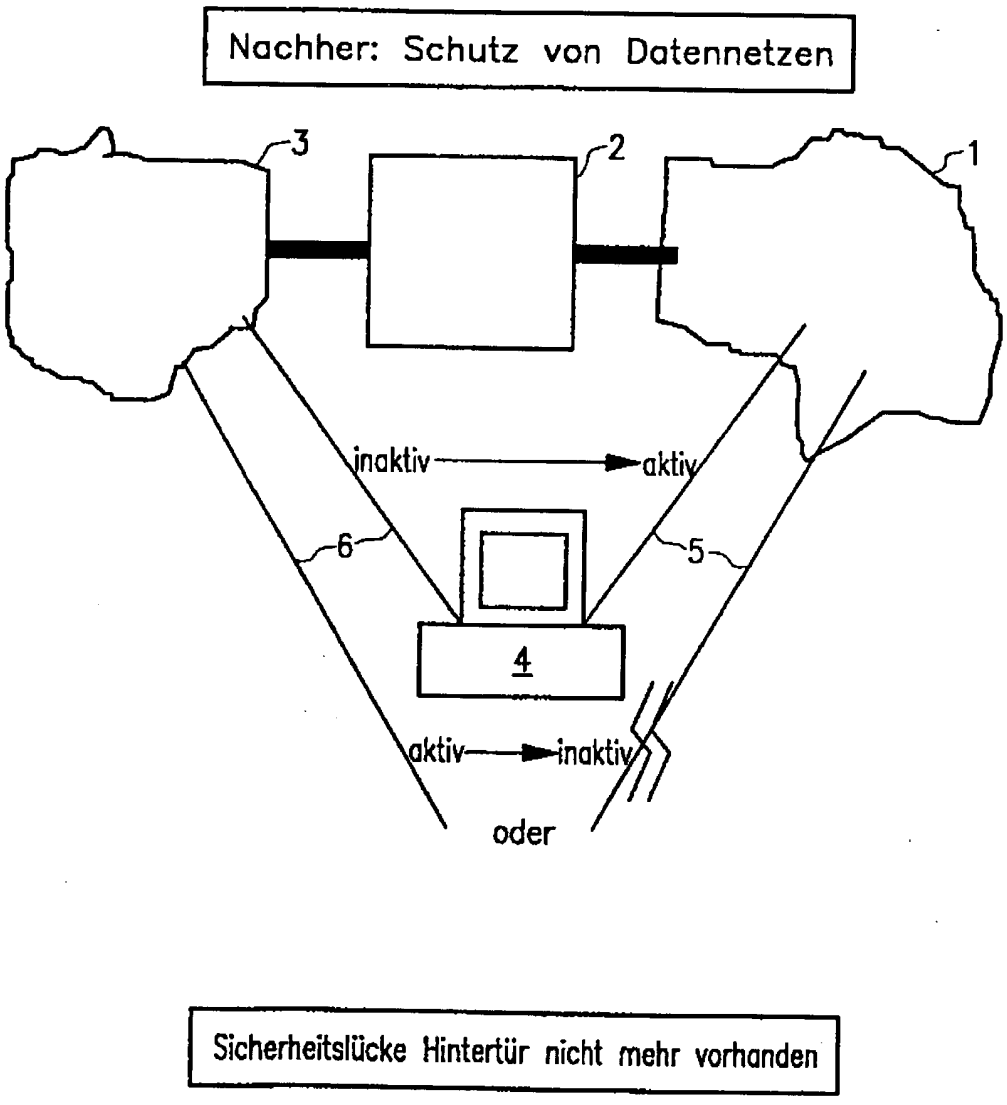

Nachher: Schutz von Datennetzen
3
2
1
inaktiv
aktiv
6
5
4
aktiv
inaktiv
oder
Sicherheitslücke Hintertür nicht mehr vorhanden

FIG. 1

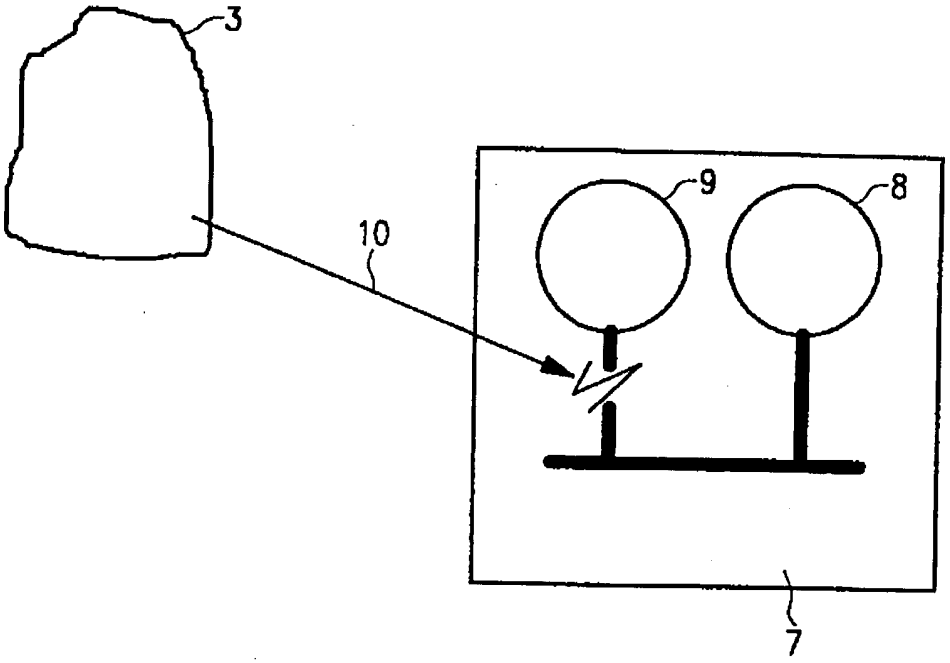


FIG.2

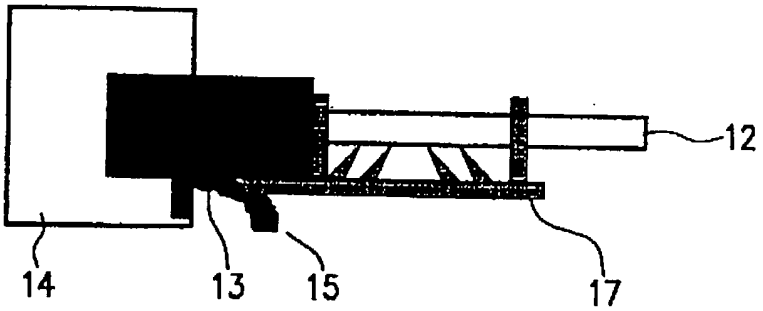


FIG.3

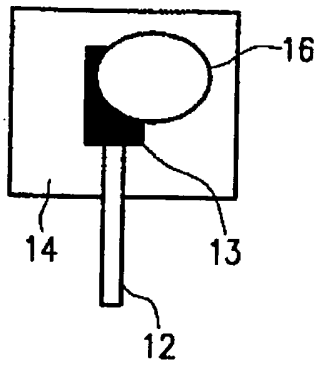

16
14
13
12

FIG.4

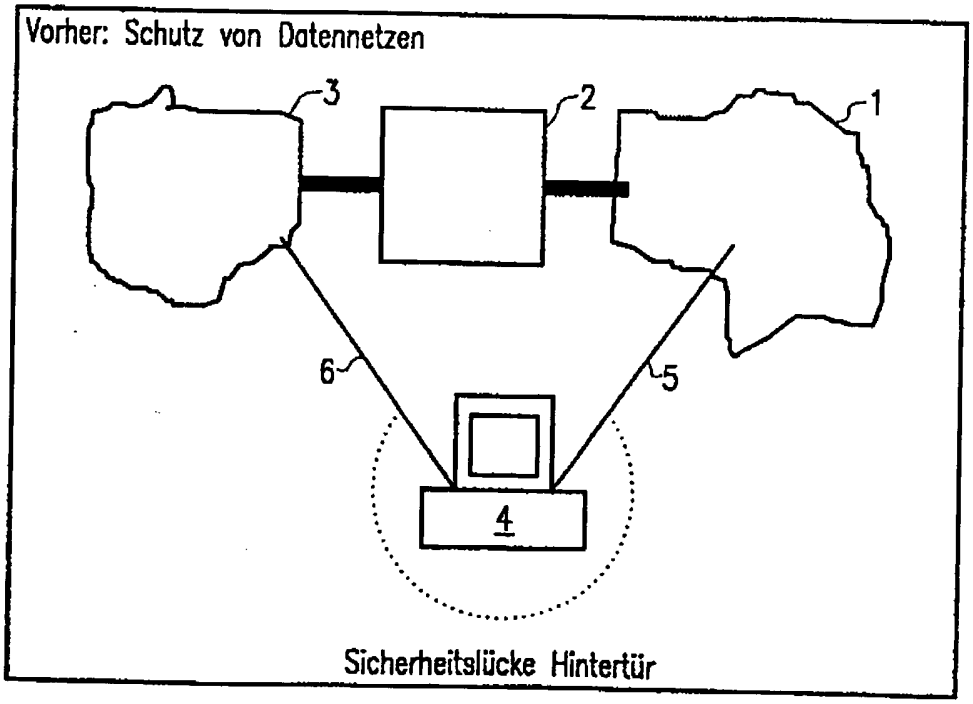

Vorher: Schutz von Datennetzen
3
2
1
6
5
4
Sicherheitslücke Hintertür

FIG.5

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/EP 99/03088

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/22 H04L12/12 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 98 25372 A (VOLTAIRE ADVANCED DATA SECURIT) 11 June 1998 (1998-06-11) abstract page 10, line 4 - line 9 page 11, line 24 - line 27 page 13, line 9 - line 14 page 16, line 14 - page 17, line 29 page 20, line 13 - page 25, line 27 claims 1,2,7,9	1-12,15, 22-25, 28-30
X	WO 97 16782 A (HOLBOROW LESLIE CHRISTOPHER) 9 May 1997 (1997-05-09)	22-29
A	abstract page 1, line 21 - line 27 page 2, line 2 - page 3, line 1 page 4, line 11 - line 24	1-6,11, 15

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 July 1999	09/08/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Karavassilis, N

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/EP 99/03088

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 198 806 A (LORD JOHN J) 30 March 1993 (1993-03-30) the whole document "in particular column 3, lines 51-53"	1-3, 7-11,14, 15, 22-24,27
X	US 4 484 306 A (KULCZYCKYJ ANTIN U ET AL) 20 November 1984 (1984-11-20) column 4, line 6 - column 5, line 47 "in particular column 4, lines 63-65"	1-4,6-8, 10,15, 22-27

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

..formation on patent family members

Inter nal Application No
PCT/EP 99/03088

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9825372 A	11-06-1998	AU 5065998 A	29-06-1998
WO 9716782 A	09-05-1997	AU 7314096 A	22-05-1997
		GB 2306862 A	07-05-1997
US 5198806 A	30-03-1993	NONE	
US 4484306 A	20-11-1984	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/EP 99/03088

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L12/22 H04L12/12 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	WO 98 25372 A (VOLTAIRE ADVANCED DATA SECURIT) 11. Juni 1998 (1998-06-11) Zusammenfassung Seite 10, Zeile 4 - Zeile 9 Seite 11, Zeile 24 - Zeile 27 Seite 13, Zeile 9 - Zeile 14 Seite 16, Zeile 14 - Seite 17, Zeile 29 Seite 20, Zeile 13 - Seite 25, Zeile 27 Ansprüche 1,2,7,9	1-12,15, 22-25, 28-30
X	WO 97 16782 A (HOLBOROW LESLIE CHRISTOPHER) 9. Mai 1997 (1997-05-09)	22-29
A	Zusammenfassung Seite 1, Zeile 21 - Zeile 27 Seite 2, Zeile 2 - Seite 3, Zeile 1 Seite 4, Zeile 11 - Zeile 24	1-6,11, 15

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
30. Juli 1999	09/08/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Karavassilis, N

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/EP 99/03088

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 198 806 A (LORD JOHN J) 30. März 1993 (1993-03-30) das ganze Dokument "insbesondere Spalte 3, Zeile 51-53"	1-3, 7-11,14, 15, 22-24,27
X	US 4 484 306 A (KULCZYCKYJ ANTIN U ET AL) 20. November 1984 (1984-11-20) Spalte 4, Zeile 6 - Spalte 5, Zeile 47 "insbesondere Spalte 4, Zeile 63-65"	1-4,6-8, 10,15, 22-27

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 99/03088

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9825372 A	11-06-1998	AU 5065998 A	29-06-1998
WO 9716782 A	09-05-1997	AU 7314096 A	22-05-1997
		GB 2306862 A	07-05-1997
US 5198806 A	30-03-1993	KEINE	
US 4484306 A	20-11-1984	KEINE	